SOLUTION DE CRYPTAGE DISK

TRUECRYPT

Ce guide décrit l'installation de truecrypt sous Windows xp ainsi que la création d'un volume crypté.

Agence Nationale de la Sécurité Informatique

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Gestion de document

Version	Date	Modification apportée
0.1	08/06/2009	Première version
0.2	05/02/2010	Maj. de version et de rédaction de guide.

Document Publique Document Interne

PLAN

Présentation 3
1. Installation 3
2. Création de volume 6
3. Monter un disque 13
4. Démonter un disque 18

PRESENTATION

TrueCrypt est un logiciel libre et gratuit de chiffrement à la volée, fonctionnant sur Microsoft Windows XP/2000/2003/Vista (32-bit et 64-bit), Mac OS X et Linux.

Il permet de créer un disque virtuel chiffré (volume TrueCrypt) contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt peut aussi chiffrer une partition entière ou un périphérique, comme une disquette ou une clé USB.

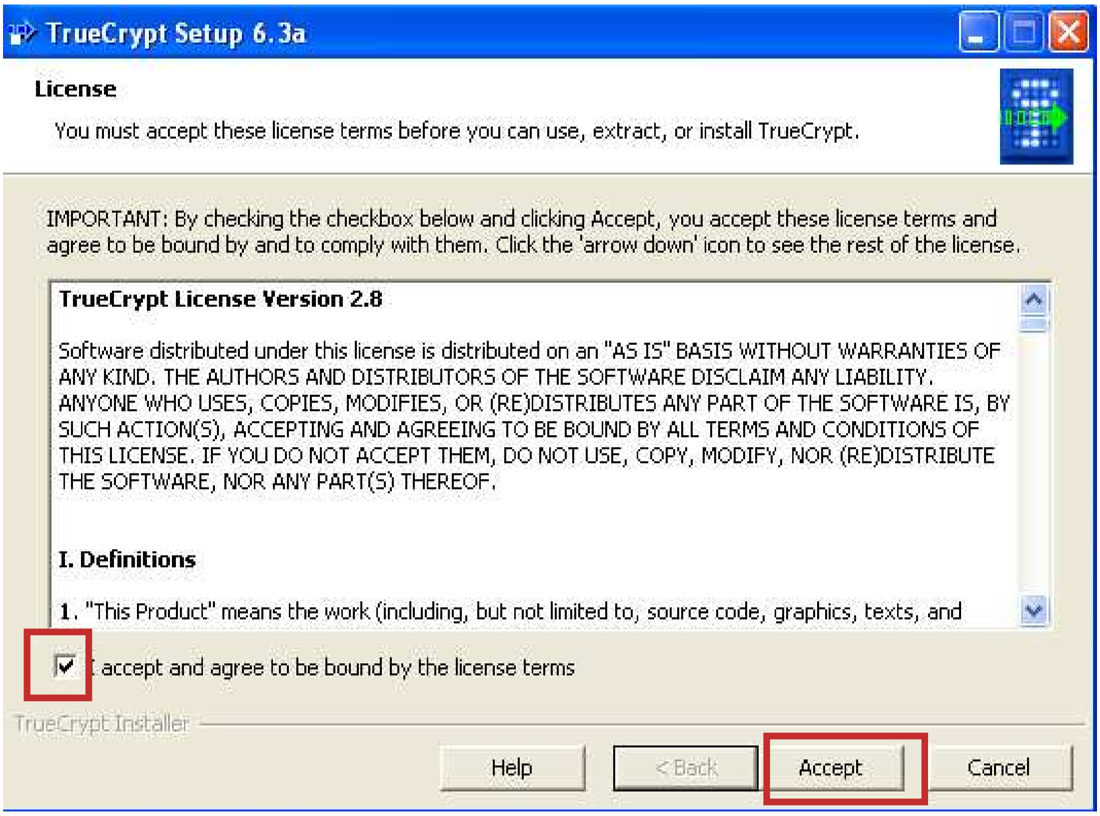
Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré. Il est ainsi possible, par exemple, d'en réparer le système de fichiers avec chkdsk, ou de défragmenter les volumes créés par TrueCrypt une fois montés.

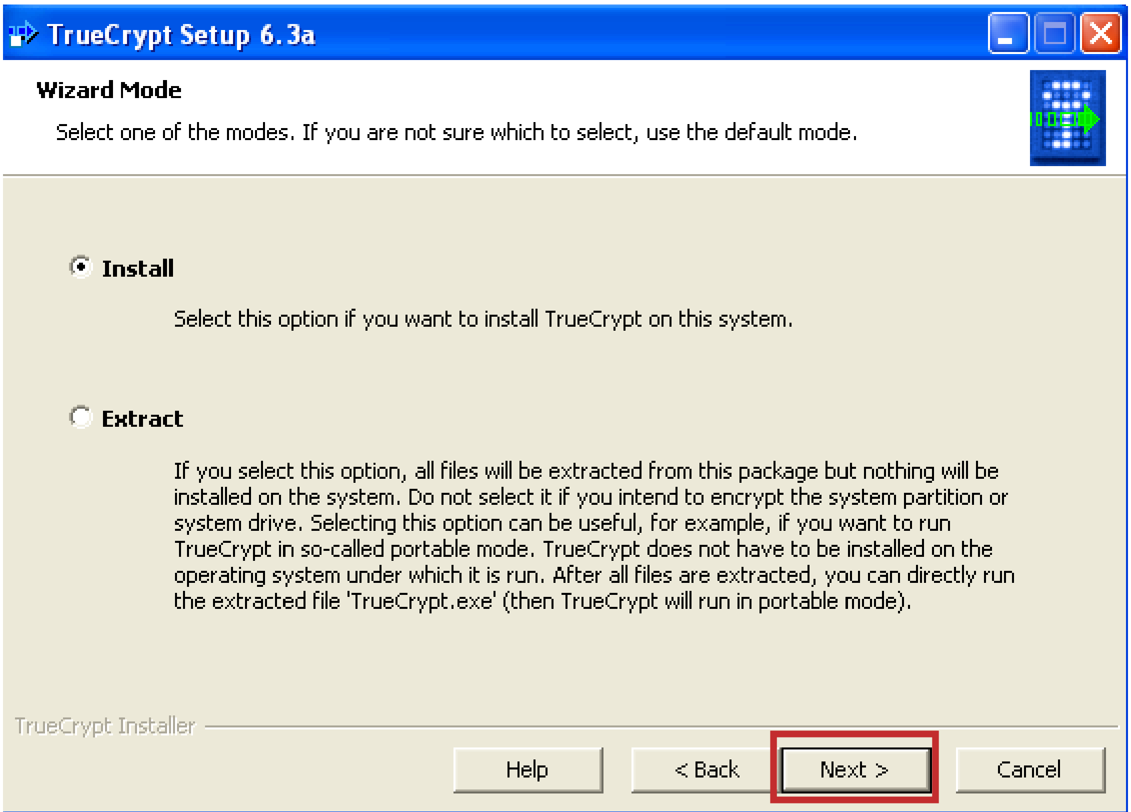
Le chiffrement à la volé signifie que le volume chiffré est rattaché à l'arborescence du système de fichiers comme s'il était un disque dur physique (ou un périphérique amovible), rendant ainsi son contenu accessible de la même manière que le contenu des volumes non chiffrés.

Vous pouvez le télécharger depuis son site officiel : http://www.truecrypt.org/downloads

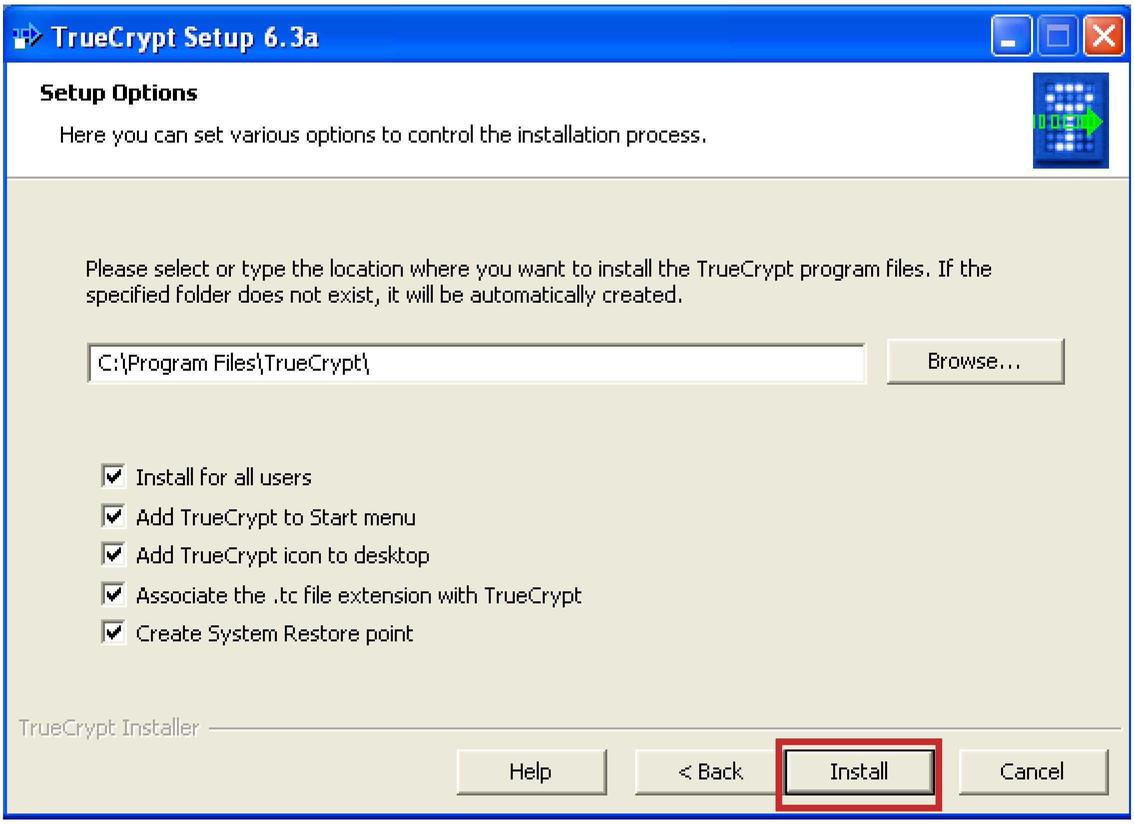
1. INSTALLATION

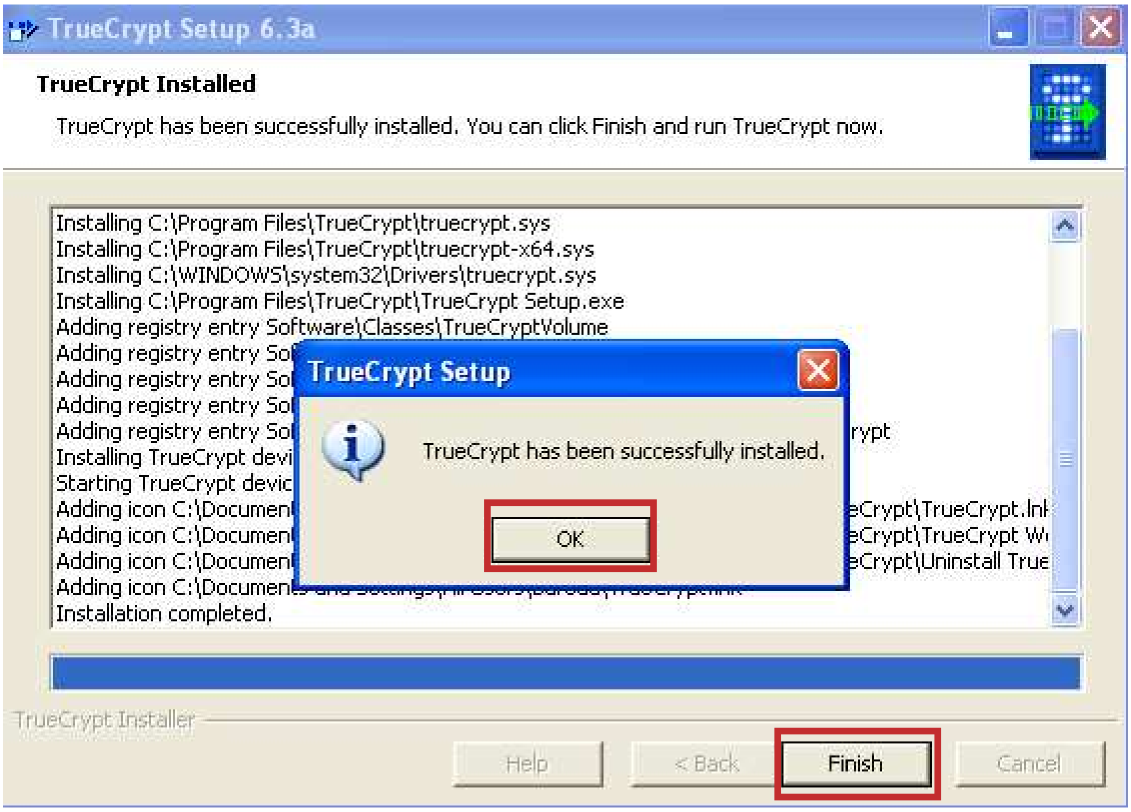
- Après avoir téléchargé le fichier « Truecrypt Setup 6.3a.exe » et exécutez-le.





- Une fois l'interface de l'installation apparaît, vous êtes invité à choisir le chemin de l'installation ainsi que quelques paramètres.





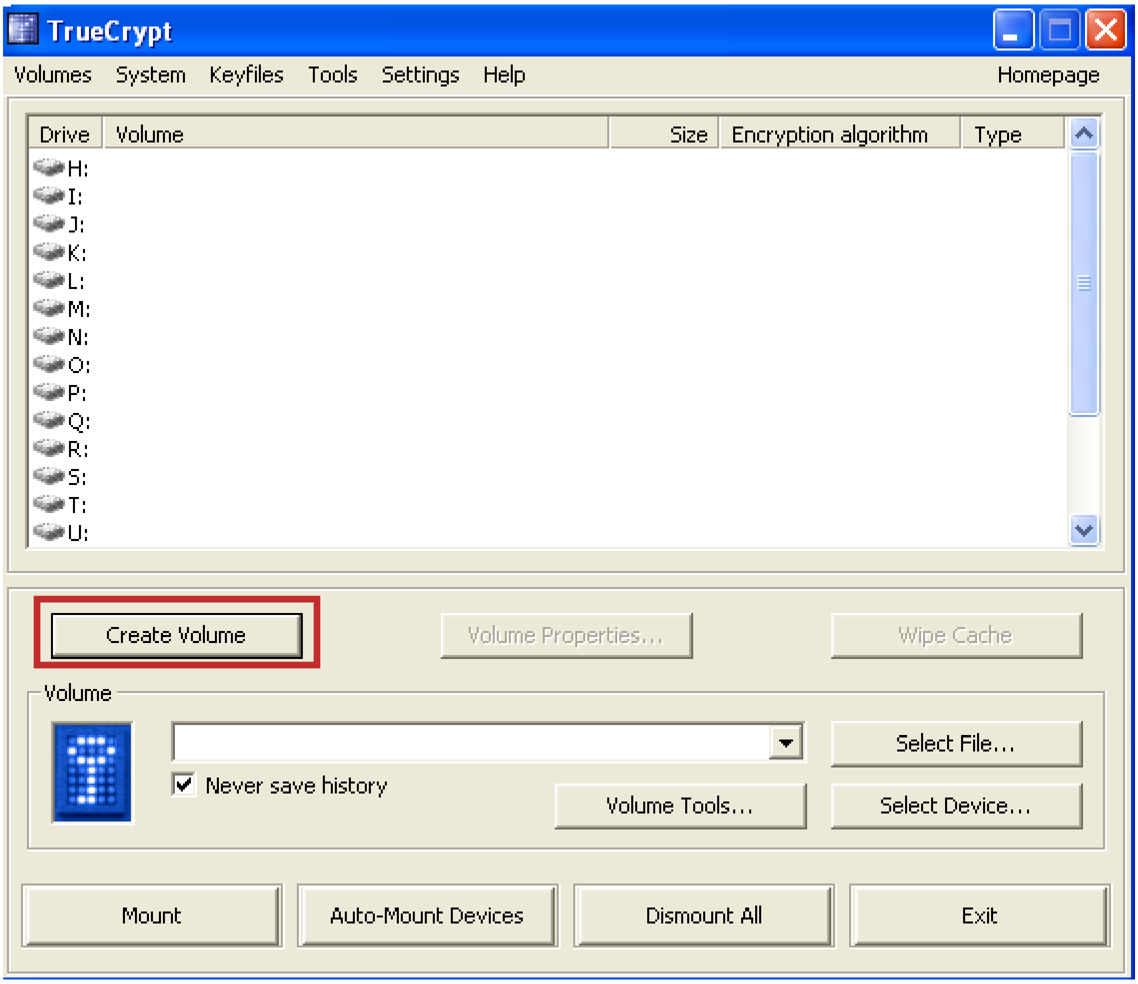
TrueCrypt est livré avec un manuel d'utilisation en anglais, pendant la première installation réalisé vous serez inviter à lire le manuel.

2. CREATION DE VOLUME

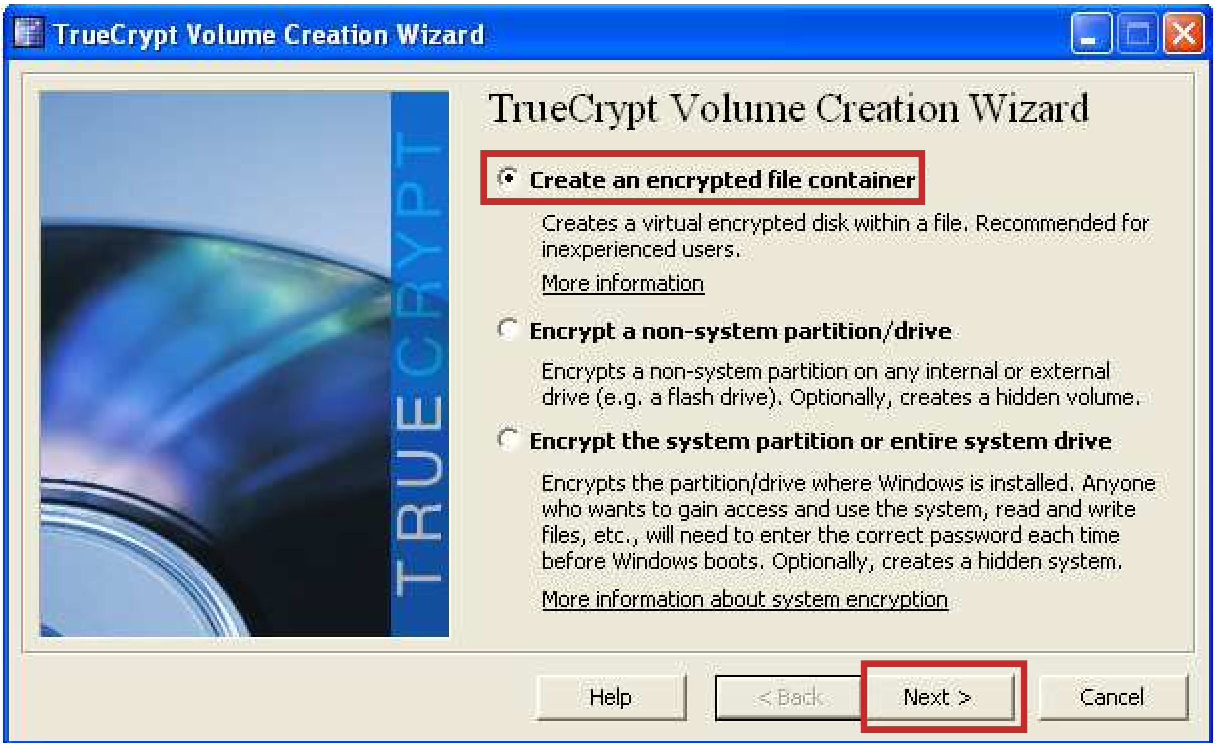
TrueCrypt vous permet de :

- ✓ créer un volume virtuel
- ✓ chiffrer un périphérique tel qu'une clé USB
- ✓ chiffrer une partition système ou un disque dur entier, c'est à dire une partition ou un lecteur sur lequel Windows est installé.

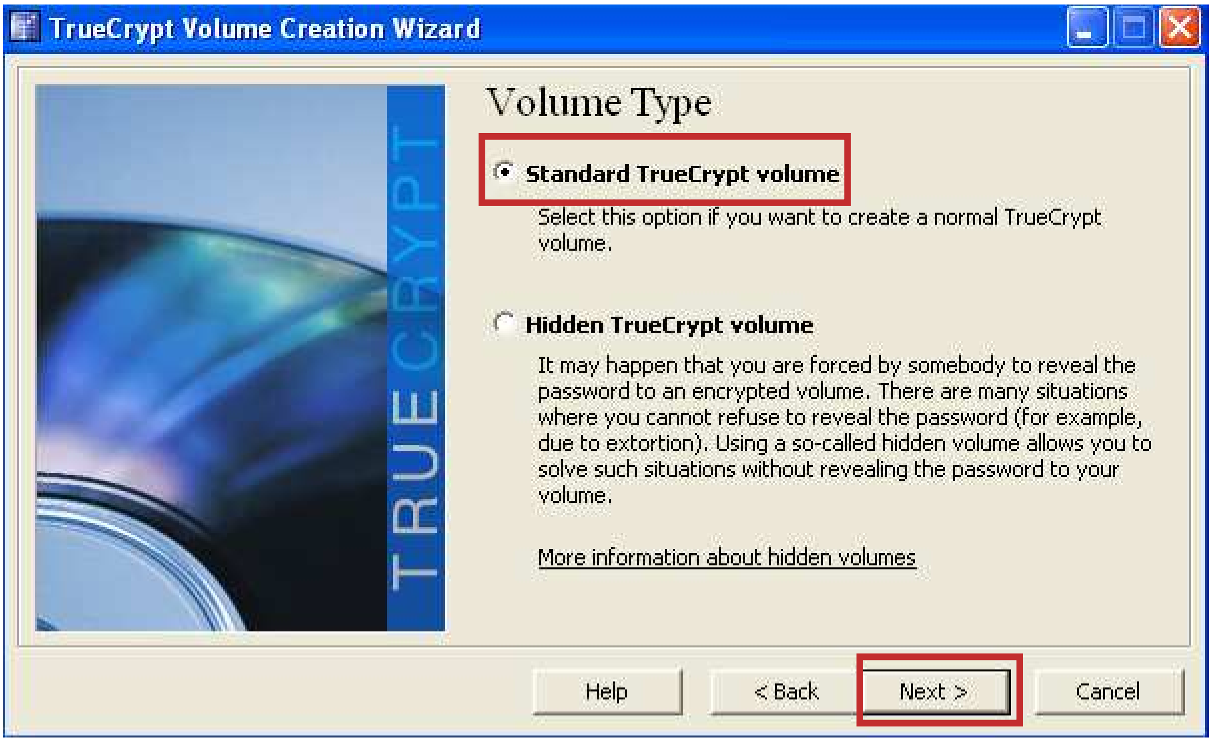
- Cliquez sur « ***create volume*** »



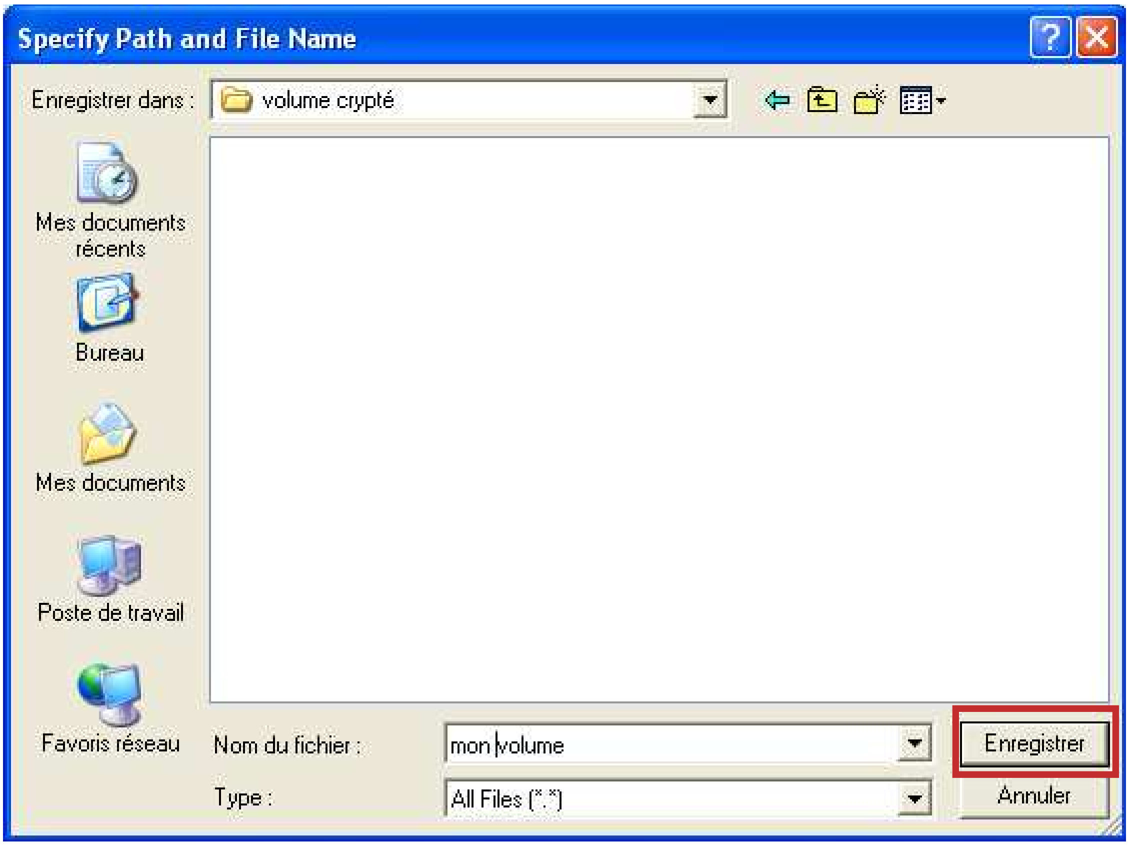
- Dans notre tutorial nous allons créer un volume virtuel qui sera ensuite monté en étant un disque physique.

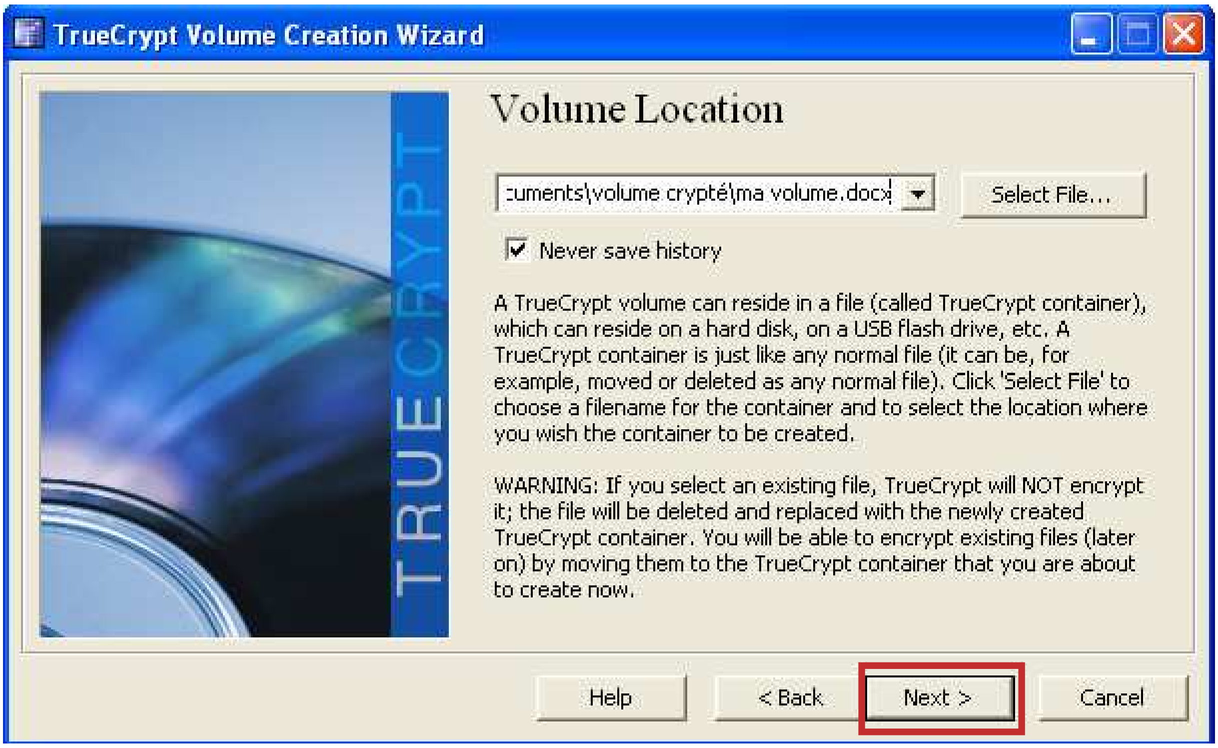


- Dans cette étape, vous avez le choix de créer un standard ou un volume TrueCrypt caché. Dans ce guide, nous allons choisir la première option, c'est de créer un volume TrueCrypt standard.



- Nous allons créer notre volume TrueCrypt dans le dossier « C:\Mes Documents\volume crypté » et le nom du volume (conteneur) sera « mon volume » (comme on peut le voir dans la capture d'écran ci-dessous). Notez que le fichier Mon volume n'existe pas encore, Truecrypt le créera.
- IMPORTANT: Notez que Truecrypt ne cryptera pas les fichiers existants. Si vous sélectionnez un fichier existant, il sera écrasé et remplacé par le volume nouvellement créé. Vous serez en mesure de chiffrer les fichiers existants (plus tard) en les déplaçant vers le volume Truecrypt que nous sommes en train de le créer.





- Ici, vous pouvez choisir un algorithme de chiffrement et un algorithme de hachage pour le volume. Truecrypt utilise l'un des algorithmes de cryptage suivants et il peut même combiner entre eux.

  - AES
  - Serpent
  - Twofish

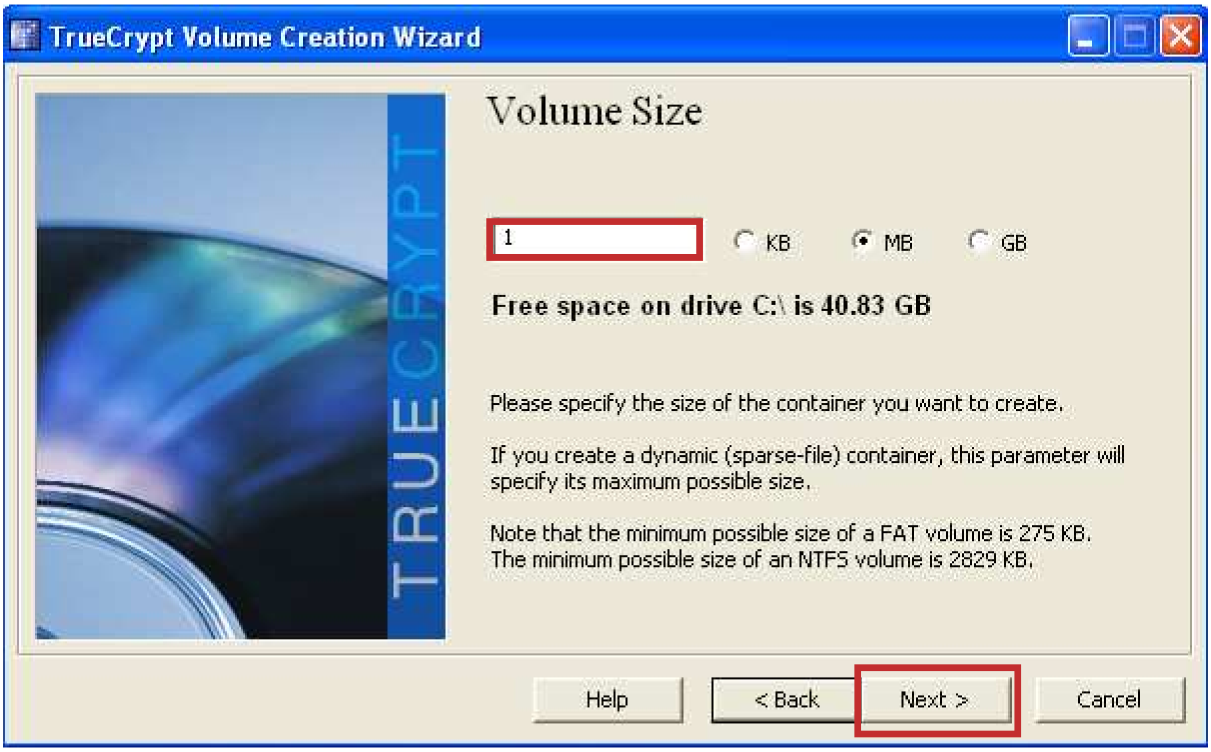
  Comme il utilise les algorithmes de hachage afin d'être utiliser pour générer « *Random Number* » plus tard.

  - RIPEMD-160
  - SHA-512
  - Whirlpool

  Vous pouvez faire une petite recherche sur internet sur le fonctionnement de chaque algorithme et si vous ne savez pas quoi choisir ici, vous pouvez utiliser les paramètres par défaut et cliquez sur Suivant



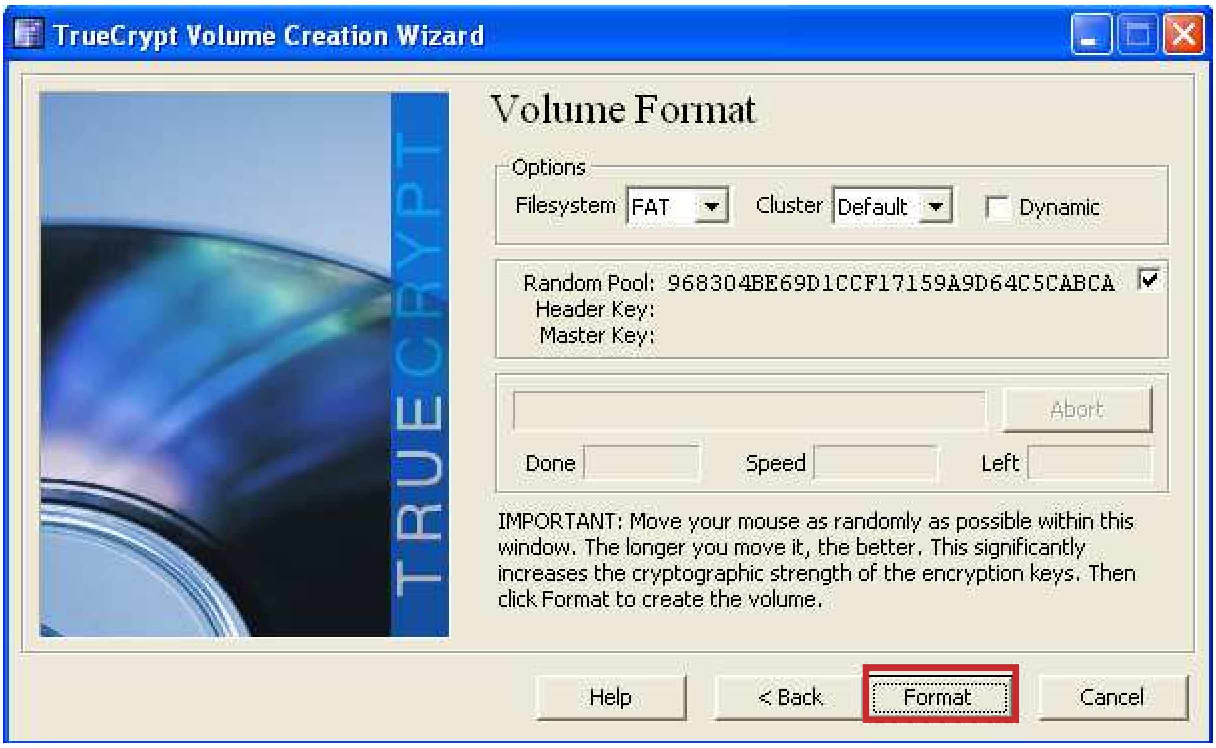
- Ici, nous précisons que la taille de notre container Truecrypt soit à 1 mégaoctet. Une fois que vous tapez la taille souhaitée dans le champ de saisie cliquez sur Suivant.



- C'est l'une des étapes les plus importantes. Ici, vous devez choisir un bon mot de passe pour le volume.
- Lire attentivement les informations affichées dans la fenêtre de l'assistant de ce qui est considéré comme un bon mot de passe.
- Après avoir choisi un mot de passe, tapez-le dans le champ de saisie, puis cliquez sur Suivant.



- Déplacez votre souris de manière aléatoire que possible dans la fenêtre Assistant de création de volumes, pendant au moins 30 secondes. Ceci augmente sensiblement le niveau de chiffrement des clés de cryptage. Ensuite Cliquez sur Format.



- Cliquez sur OK pour fermer la boîte de dialogue.



- Nous venons tout juste réussi à créer un volume Truecrypt.

- Cliquez sur Exit afin de fermer l'assistant de « Création de Volume Truecrypt ».



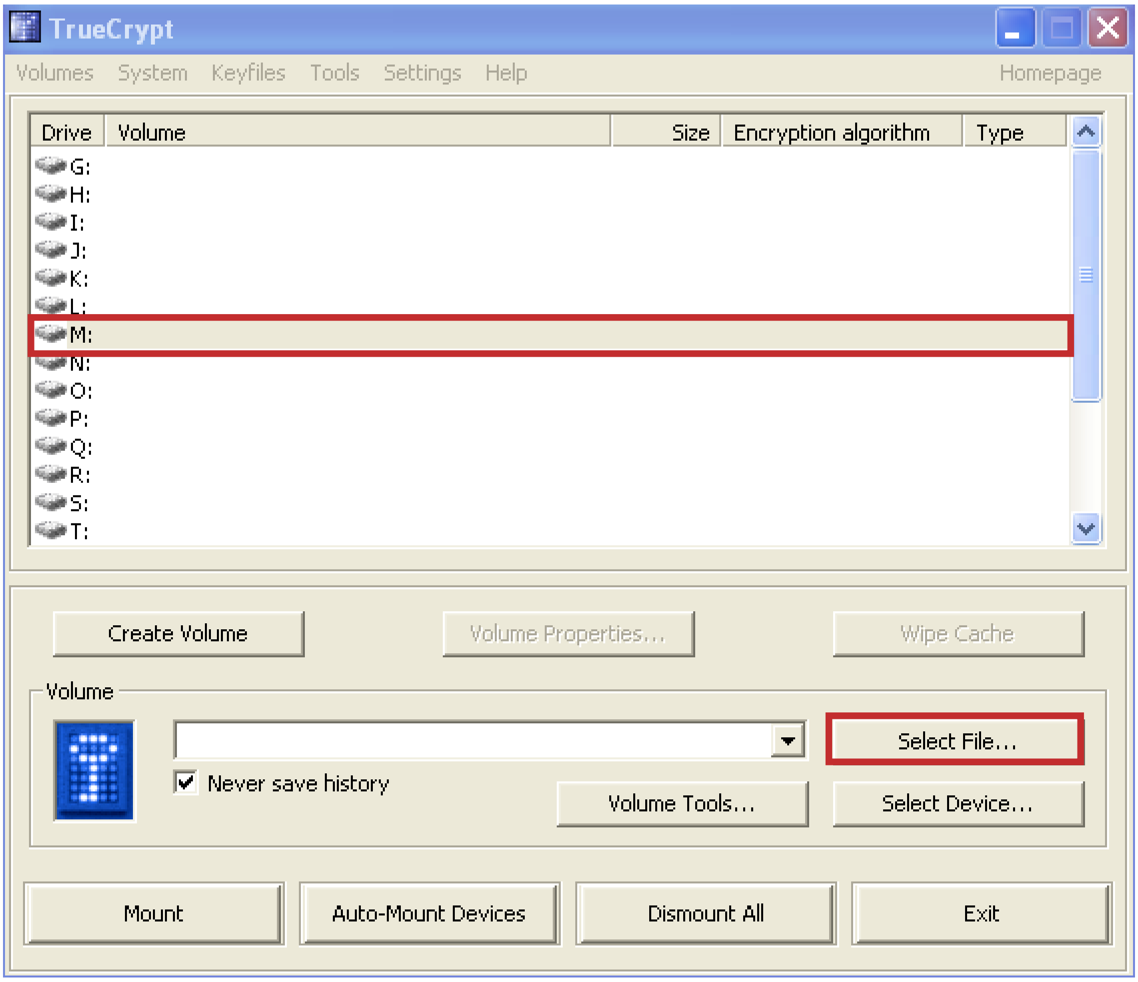
3. Monter un disque

Dans les étapes suivantes, nous allons monter le volume que nous venons de créer. Nous allons revenir à la fenêtre principale de Truecrypt.

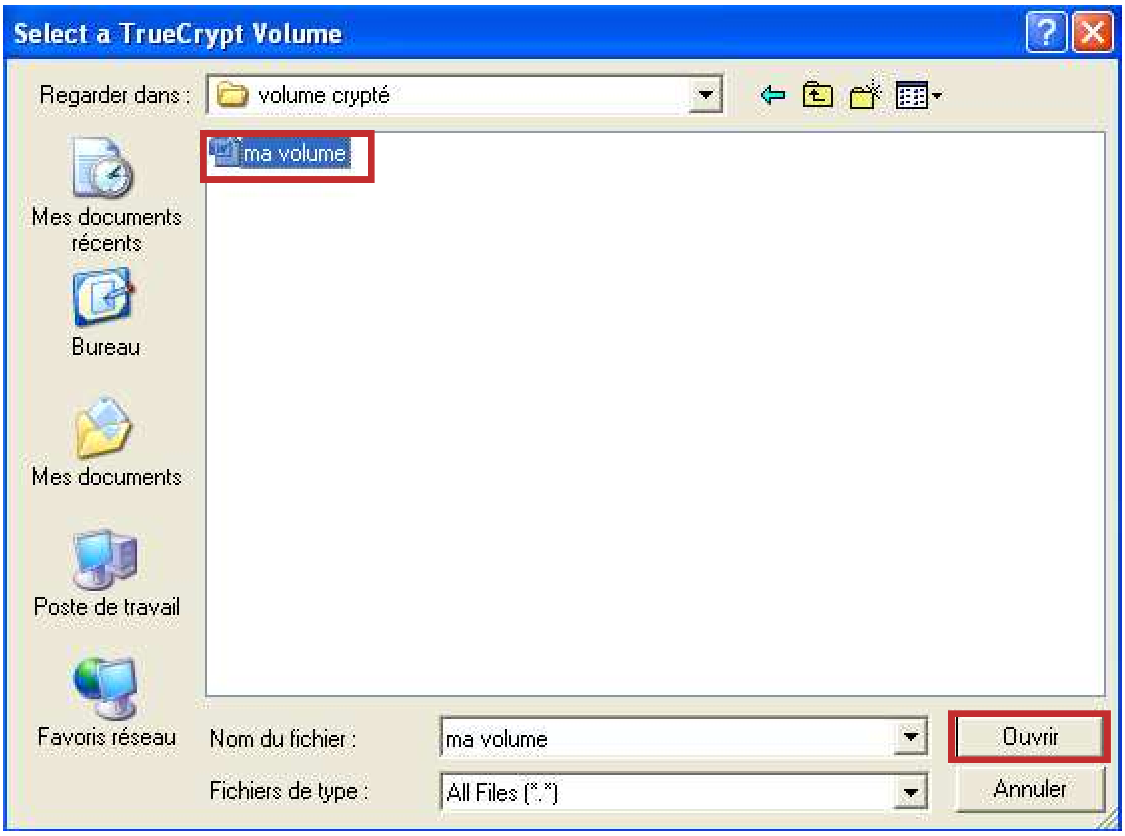
- Sélectionnez une lettre de lecteur dans la liste. Ça sera la lettre de lecteur à laquelle le volume Truecrypt sera monté.

  Note: vous pouvez choisir n'importe quelle autre lettre de lecteur disponible.

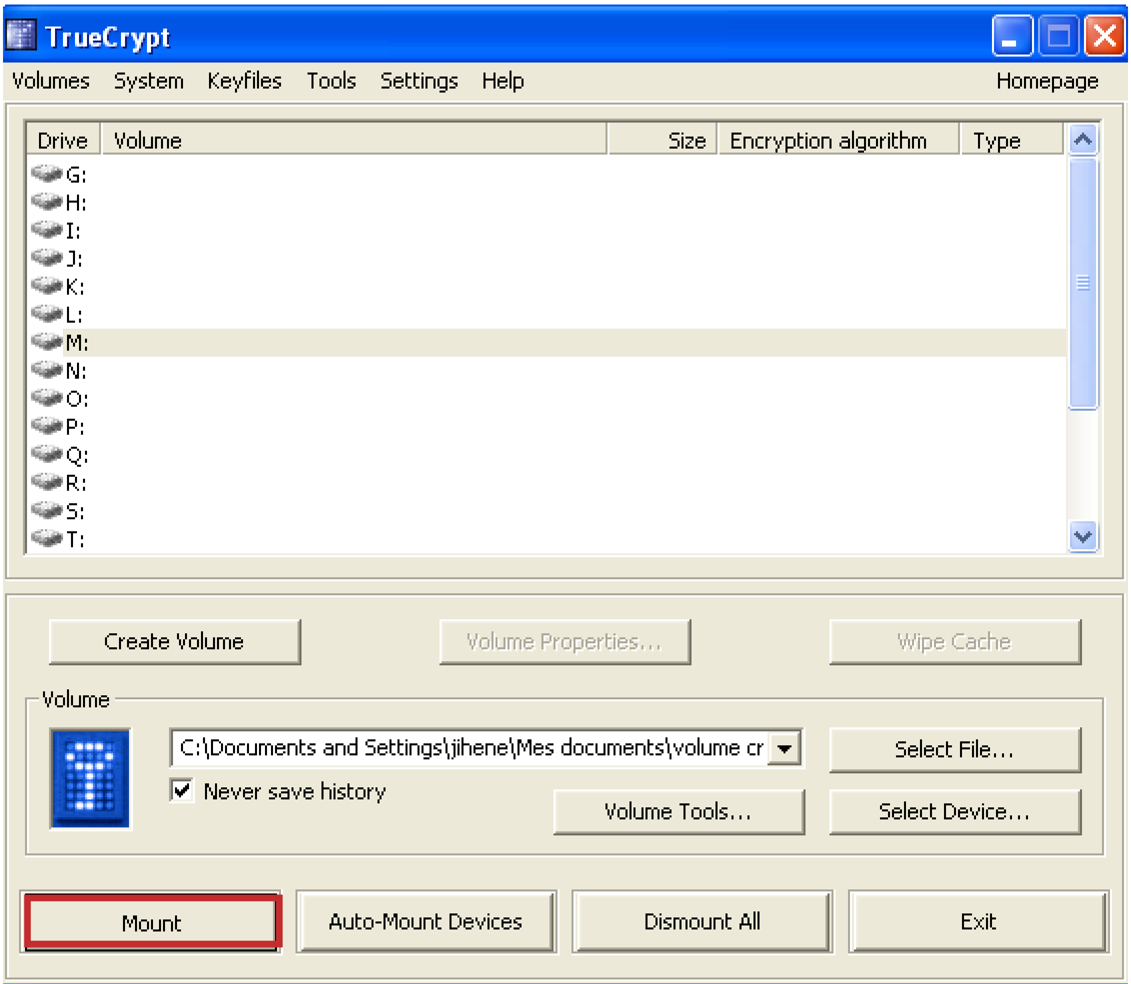
- Cliquez sur ***« Select file »***. La fenêtre du sélecteur de fichier standard devrait apparaître.



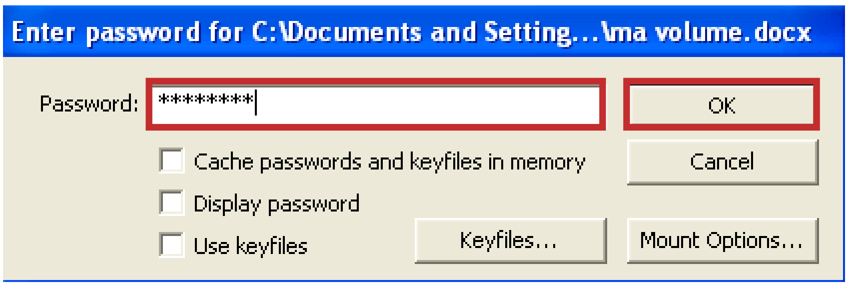
- Dans le sélecteur de fichier, naviguez jusqu'au dossier contenant le volume, sélectionnez le et cliquez sur Ouvrir.



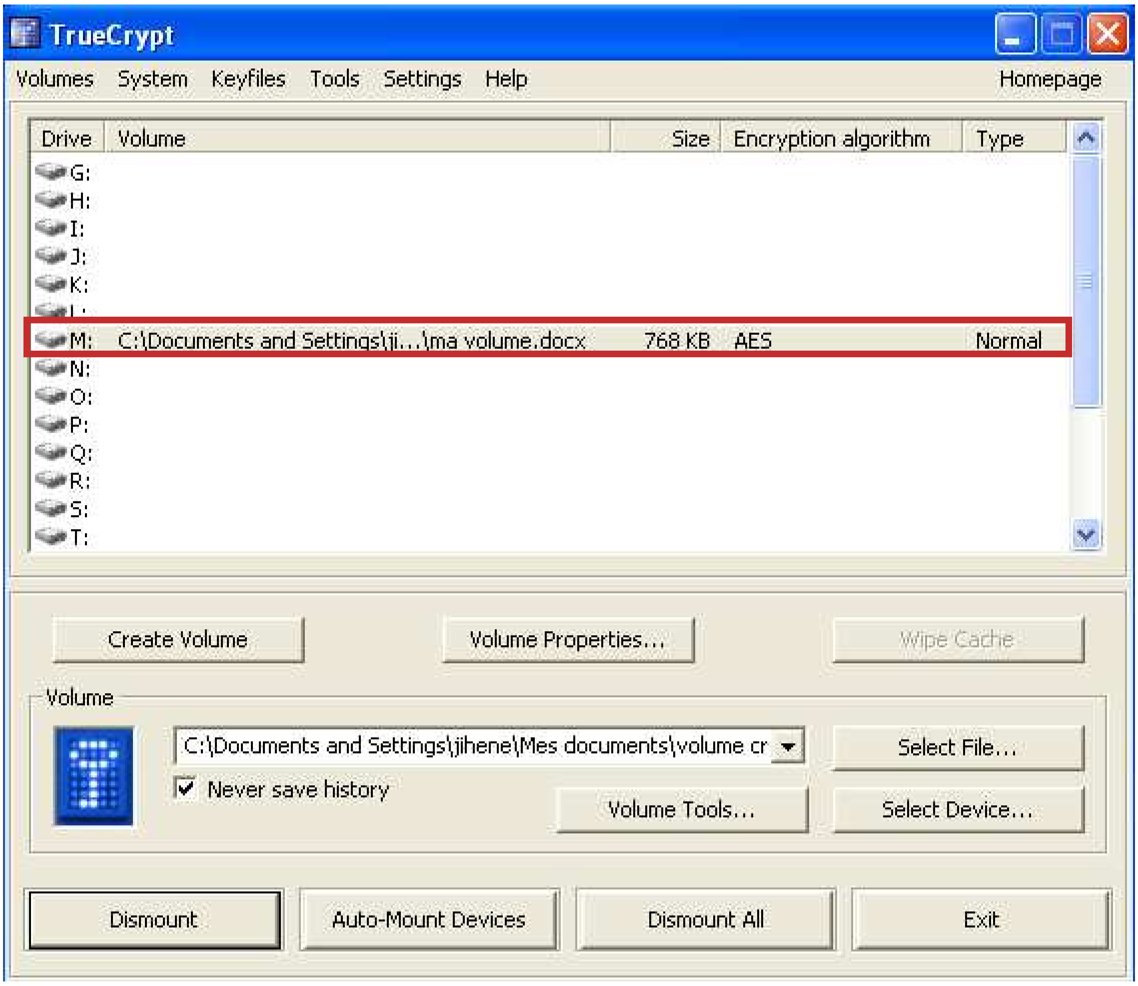
- Dans la fenêtre principale de Truecrypt, cliquez sur Monter. La fenêtre d'invite de dialogue de Mot de passe devrait apparaître.

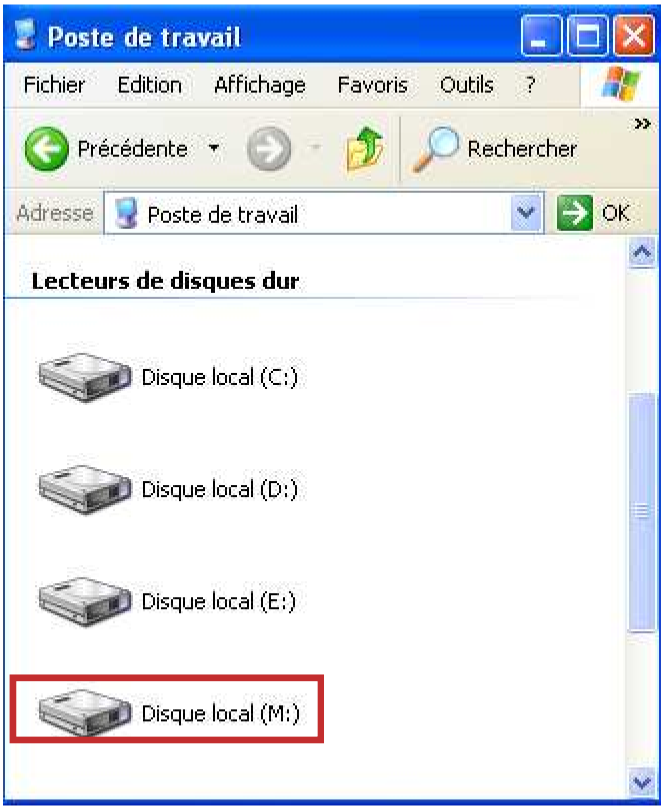


- Tapez le mot de passe dans le champ de saisie de mot de passe.



- Nous venons de montée avec succès le volume comme un disque virtuel « M: » Le disque virtuel est entièrement crypté (y compris les noms de fichiers, les tables d'allocation, l'espace libre, etc.) et il se comporte comme un véritable disque.
- Vous pouvez ouvrir le volume monté, par exemple, en double-cliquant sur la lettre ***« M : »*** comme il est marqué dans la capture d'écran ci-dessus.
- Vous pouvez également parcourir le volume monté dans « poste de travail ».


TrueCrypt
Volumes System Keyfiles Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
G:
H:
I:
J:
K:
M: C:\Documents and Settings\ji...\ma volume.docx 768 KB AES Normal
N:
O:
P:
Q:
R:
S:
T:
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Documents and Settings\jihene\Mes documents\volume cr
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit


Poste de travail
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Adresse
Poste de travail
OK
Lecteurs de disques dur
Disque local (C:)
Disque local (D:)
Disque local (E:)
Disque local (M:)

- Vous pouvez copier des fichiers vers et à partir du volume Truecrypt juste comme vous les copiez sur un disque normal. Les fichiers qui sont lus ou copiés à partir du volume chiffré Truecrypt sont automatiquement décryptés à la volée dans la mémoire / RAM.
- De même, les fichiers qui sont écrits ou copiés dans le volume chiffré Truecrypt sont automatiquement cryptés à la volée dans la RAM.
- Notez que : Truecrypt sauve jamais de données décryptées dans un disque. Il ne les stocke que temporairement dans la RAM (mémoire). Même lorsque le volume est monté, les données stockées dans le volume sont toujours cryptée. Lorsque vous redémarrez Windows ou éteignez votre ordinateur, le volume sera démonté et tous les fichiers stockés sur elle ne seront pas accessible.

4. DEMONTER UN DISQUE

- Si vous souhaitez fermer le volume et rendre tous les fichiers stockés dedans inaccessible, alors démonter le volume comme suit :

